Comprendre l'affectation dynamique des SGT/L2VNID sur SDA sans fil

Table des matières

Introduction

Ce document décrit le processus d'attribution de SGT dynamique et de L2VNID sur les SSID sans fil 802.1x activés par le fabric.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- RADIUS (Remote Authentication Dial-In User Service)
- Contrôleur LAN sans fil (WLC)
- Identity Services Engine (ISE)
- Balise de groupe de sécurité (SGT)
- L2VNID (identifiant de réseau virtuel de couche 2)
- Sans fil compatible avec le fabric d'accès SD (SDA FEW)
- Protocole LISP (Locator/ID Separation Protocol)
- Réseau local extensible virtuel (VXLAN)
- Plan de contrôle du fabric (CP) et noeud de périphérie (EN)
- Catalyst Center (CatC, anciennement Cisco DNA Center)

Composants utilisés

WLC 9800 Cisco IOS® XE version 17.6.4

Cisco IOS® XE

ISE version 2.7

CatC version 2.3.5.6

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

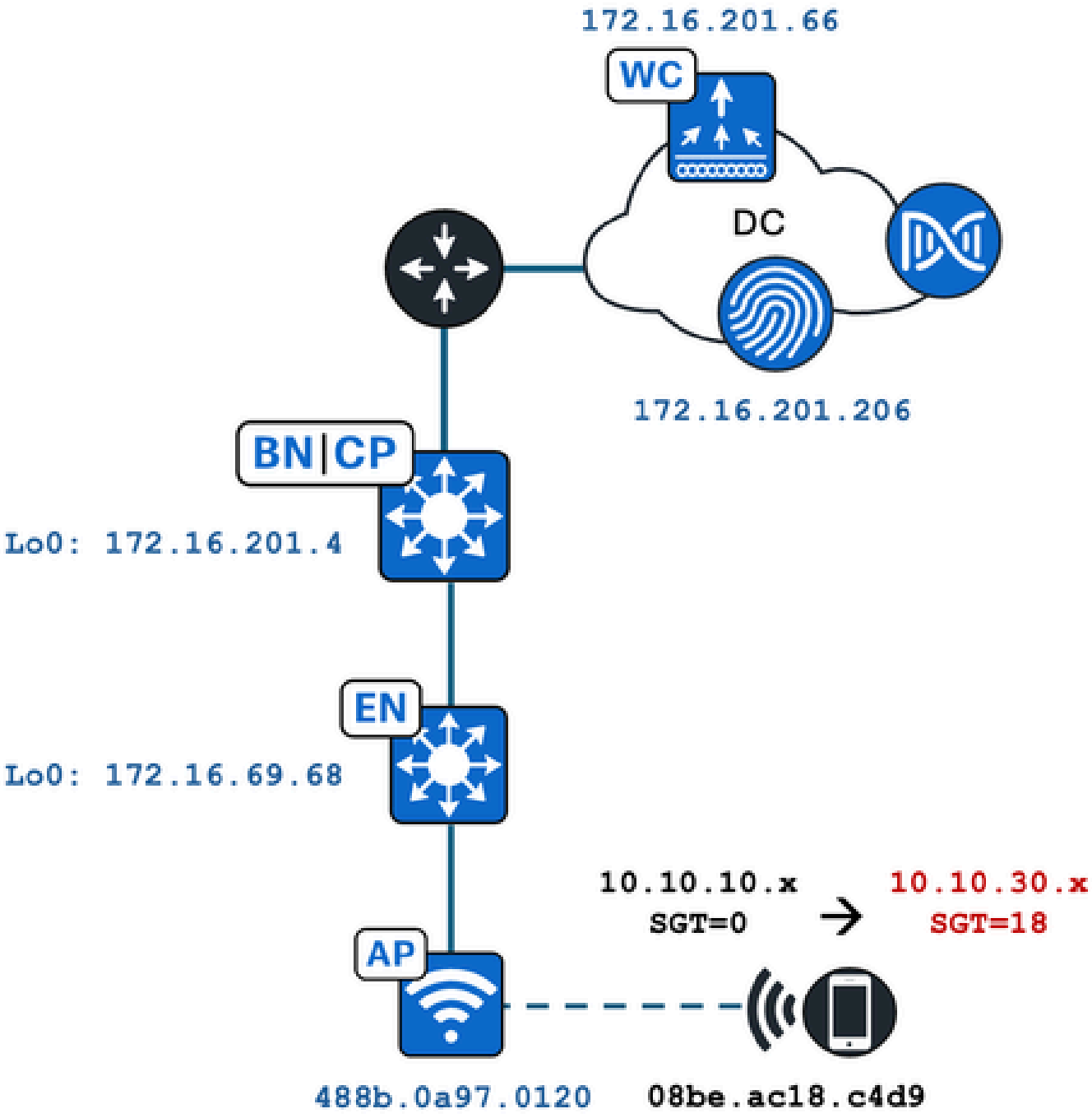
L'un des aspects clés de SD-Access est la microsegmentation au sein d'un VLAN réalisée via les groupes évolutifs.

Les balises SGT peuvent être attribuées de manière statique par WLAN ou SSID activés par le fabric (bien qu'elles ne soient pas identiques, leur différence n'a pas d'incidence sur l'objectif principal de ce document, de sorte que nous utilisons indifféremment les deux termes pour la même signification afin d'améliorer la lisibilité). Cependant, dans de nombreux déploiements réels, il arrive souvent que des utilisateurs se connectant au même WLAN nécessitent un ensemble différent de stratégies ou de paramètres réseau. En outre, dans certains scénarios, il est nécessaire d'allouer différentes adresses IP à des clients spécifiques au sein du même WLAN de fabric pour leur appliquer des stratégies IP spécifiques ou répondre aux exigences d'adressage IP de l'entreprise. L2VNID (identifiant de réseau virtuel de couche 2) est le paramètre que l'infrastructure FEW utilise pour placer les utilisateurs sans fil dans différentes plages de sous-réseaux. Les points d'accès envoient le L2VNID dans l'en-tête VxLAN au noeud de périphérie de fabric (EN), qui le met ensuite en corrélation avec le VLAN L2 correspondant.

Pour obtenir cette granularité au sein du même WLAN, l'affectation de SGT dynamique et/ou de L2VNID est exploitée. Le WLC collecte les informations d'identité du point d'extrémité, les envoie à ISE pour authentification, qui les utilise pour correspondre à la stratégie appropriée à appliquer à ce client et renvoie les informations SGT et/ou L2VNID une fois l'authentification réussie.

Topologie

Pour comprendre le fonctionnement de ce processus, nous avons développé un exemple à l’aide de cette topologie de TP :



Dans cet exemple, le WLAN est configuré de manière statique avec :

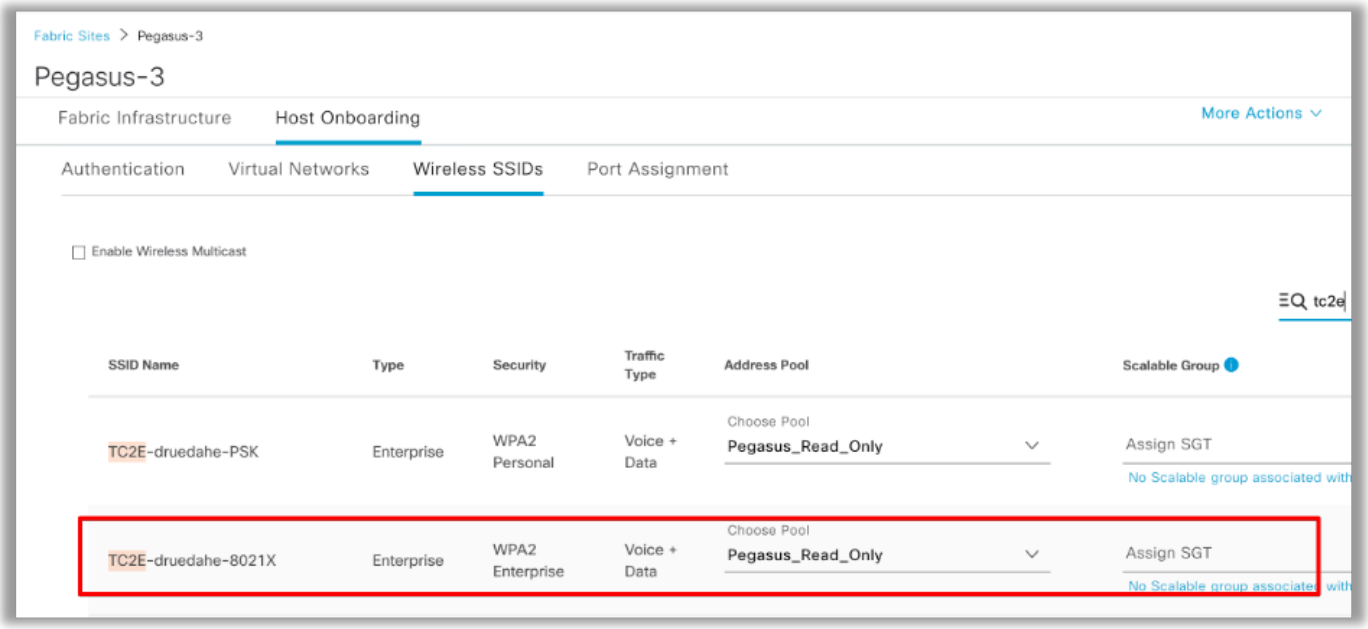
- L2VNID = 8198 / Nom du pool IP = Pegasus_Read_Only —> VLAN 1030 (10.10.10.x)
- Pas de SGT

Le client sans fil qui s'y connecte obtient dynamiquement les paramètres suivants :

- L2VNID = 8199 / Nom du pool IP = 10_10_30_0-READONLY_VN —> VLAN 1031 (10.10.30.x)
- SGT = 18

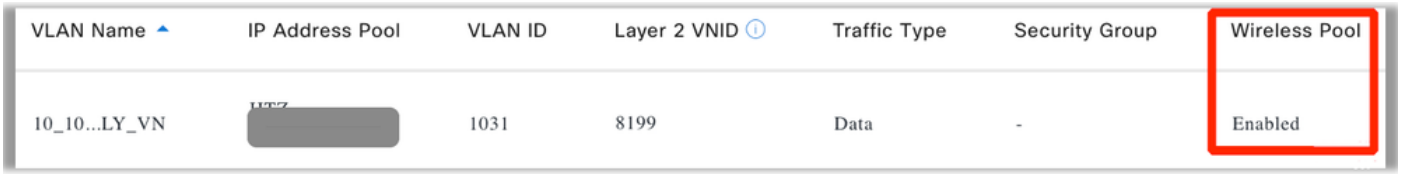
Configuration

Tout d'abord, nous devons identifier le WLAN concerné et vérifier comment il est configuré. Dans cet exemple, le SSID « TC2E-druedahe-802.1x » est utilisé. Au moment de la rédaction de ce document, le SDA n'est pris en charge que par CatC, nous devons donc vérifier ce qui y est configuré. Sous Provisioning/SD-Access/Fabric Sites/<specific Fabric site>/Host Onboarding/Wireless SSID :



Le SSID a le pool d'adresses IP nommé « Pegasus_Read_Only » qui lui est mappé et n'a pas de SGT attribué statiquement, ce qui signifie SGT=0. Cela signifie que, si un client sans fil se connecte et s'authentifie avec succès sans qu'ISE ne renvoie aucun attribut pour l'affectation dynamique, c'est ce que sont les paramètres du client sans fil.

Le pool qui est affecté dynamiquement doit être présent avant la configuration du WLC. Pour ce faire, ajoutez le pool IP en tant que « pool sans fil » dans le réseau virtuel sur le CatC :



Dans l'interface graphique utilisateur du WLC sous Configuration/Wireless/Fabric, ce paramètre reflète cette façon :

Le pool « Pegasus_Read_Only » équivaut à l'ID L2VNID 8198 et nous voulons que notre client soit sur l'ID L2VNID 8199, ce qui signifie qu'ISE doit dire au WLC d'utiliser le pool « 10_10_30_0-READONLY_VN » pour ce client. Rappelez-vous que le WLC ne contient aucune configuration pour les VLAN de fabric. Il ne connaît que les L2VNID. Chacun d'eux est ensuite mappé à un VLAN spécifique dans les EN de fabric SDA.

Vérification

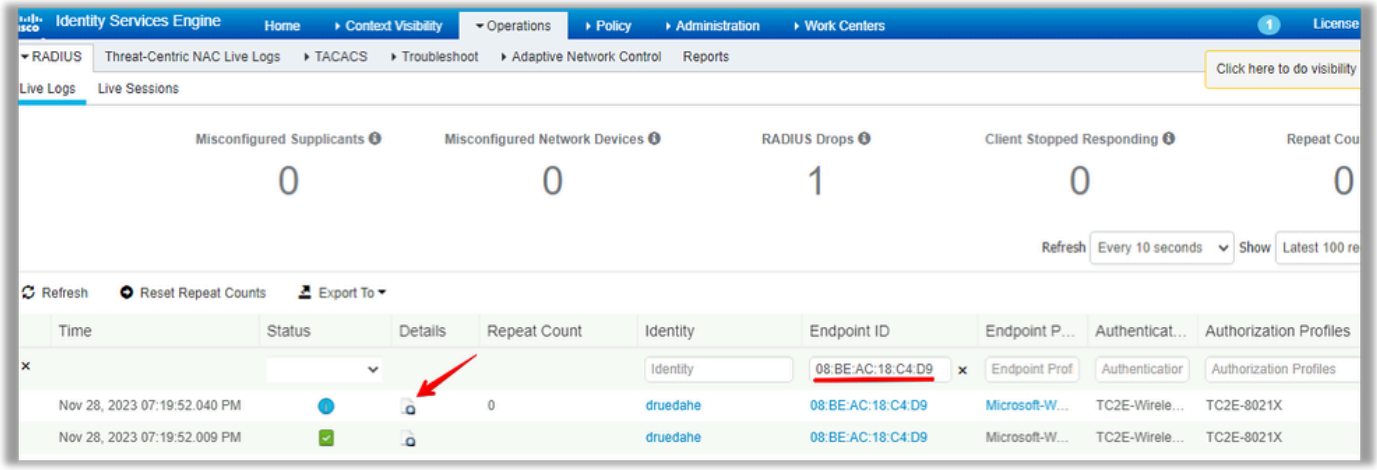
Les symptômes rapportés pour les problèmes impliquant l'affectation dynamique de SGT/L2VNID sont :

1. Les stratégies SG ne sont pas appliquées sur les clients sans fil qui se connectent à un WLAN spécifique. (Problème d'affectation de SGT dynamique).
2. Les clients sans fil n'obtiennent pas d'adresse IP via DHCP ou n'obtiennent pas d'adresse IP à partir de la plage de sous-réseaux souhaitée sur un réseau local sans fil spécifique (problème d'attribution dynamique de L2VNID).

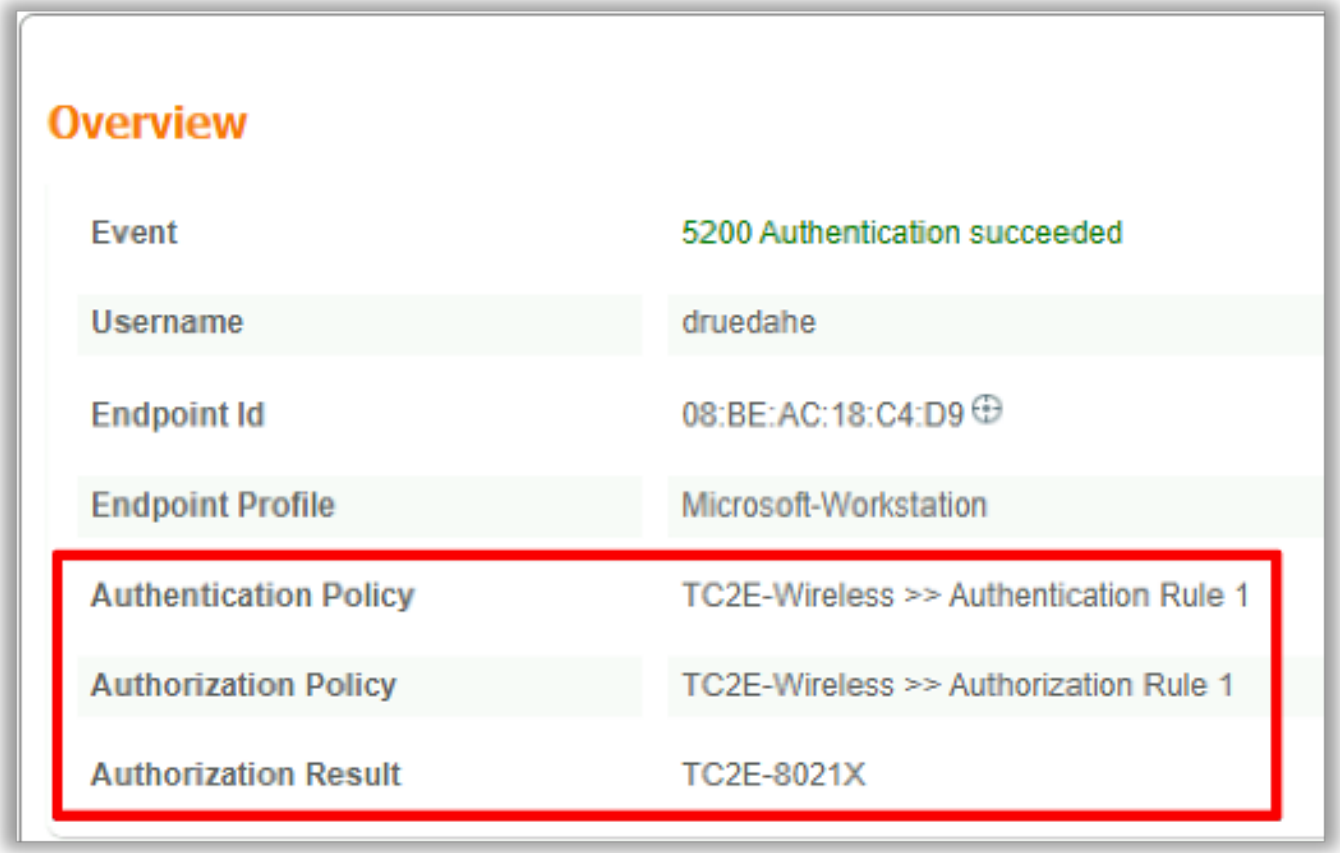
On décrit maintenant la vérification de chaque noeud pertinent dans ce processus.

Vérification ISE

Le point de départ est ISE. Accédez à l'interface utilisateur graphique ISE sous Operation/RADIUS/Live Logs/ et utilisez l'adresse MAC du client sans fil comme filtre dans le champ Endpoint ID, puis cliquez sur l'icône Details :



Il ouvre ensuite un autre onglet contenant les détails de l'authentification. Nous nous intéressons principalement à deux sections, Vue d'ensemble et Résultat :



La vue d'ensemble indique si la stratégie souhaitée a été utilisée pour cette authentification de client sans fil. Si ce n'est pas le cas, la configuration des politiques ISE doit être revue. Toutefois, cela sort du cadre de ce document.

Le résultat montre ce qui a été retourné par ISE au WLC. L'objectif est d'avoir le SGT et le L2VNID attribués dynamiquement, donc ces données doivent être incluses ici, et c'est le cas. Remarquez deux choses :

1. Le nom L2VNID est envoyé en tant qu'attribut « Tunnel-Private-Group-ID ». ISE doit renvoyer le nom (10_10_30_0-READONLY_VN) et non l'ID (8199).

2. Le SGT est envoyé en tant que « paire cisco-av ». Dans l'attribut cts : security-group-tag, notez que la valeur SGT est en hexadécimal (12) et non en ascii (18), mais qu'elles sont identiques. TC2E_Learners est le nom de SGT dans ISE en interne.

Vérification WLC

Dans le WLC, nous pouvons utiliser la commande show wireless fabric client summary pour vérifier l'état du client et la commande show wireless fabric summary pour confirmer à deux reprises la configuration du fabric et la présence du L2VNID affecté dynamiquement :

```
<#root>

eWLC#

show wireless fabric client summary

Number of Fabric Clients : 1

MAC Address    AP Name                          WLAN State              Protocol Method     L2 VNID    I
-------------------------------------------------------------------------------------------------------
08be.ac18.c4d9 DNA12-AP-01                       19   Run                 11ac     Dot1x

8199

       172.16.69.68
```

```
<#root>

eWLC4#

show wireless fabric summary


Fabric Status      : Enabled


Control-plane:
Name                              IP-address        Key                                Status
-------------------------------------------------------------------------------------------
default-control-plane             172.16.201.4      f9afa1                             Up

Fabric VNID Mapping:
  Name               L2-VNID        L3-VNID        IP Address              Subnet        Control plane n
-------------------------------------------------------------------------------------------------------
  Pegasus_APs         8196           4097           10.10.99.0          255.255.255.0      default-cont
  Pegasus_Extended     8207           0                                   0.0.0.0            default-con
  Pegasus_Read_Only     8198           0                                   0.0.0.0            default-co
```

```
10_10_30_0-READONLY_VN


8199

          0                                   0.0.0.0           default-control-plane
```

Si les informations attendues ne sont pas reflétées, nous pouvons activer RA Traces pour l'adresse MAC du client sans fil dans le WLC pour voir exactement les données reçues d'ISE. Pour plus d'informations sur l'obtention du résultat RA Traces pour un client spécifique, consultez le document suivant :

https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-6/config-guide/b_wl_17_6_cg/m_debug_ra_ewlc.html?bookSearch=true

Dans le résultat de RA Trace pour le client, les attributs envoyés par ISE sont transportés dans le paquet RADIUS Access-Accept :

<#root>

```
{wncd_x_R0-0}{1}: [radius] [21860]: (info): RADIUS: Received from id 1812/14 172.16.201.206:0,

Access-Accept

, len 425
{wncd_x_R0-0}{1}: [radius] [21860]: (info): RADIUS:  authenticator c6 ac 95 5c 95 22 ea b6 - 21 7d 8a f
{wncd_x_R0-0}{1}: [radius] [21860]: (info): RADIUS:  User-Name           [1]     10  "druedahe"
{wncd_x_R0-0}{1}: [radius] [21860]: (info): RADIUS:  Class               [25]    53  ...
{wncd_x_R0-0}{1}: [radius] [21860]: (info): 01:
{wncd_x_R0-0}{1}: [radius] [21860]: (info): RADIUS:  Tunnel-Type         [64]     6  VLAN
{wncd_x_R0-0}{1}: [radius] [21860]: (info): 01:
{wncd_x_R0-0}{1}: [radius] [21860]: (info): RADIUS:  Tunnel-Medium-Type  [65]     6  ALL_802
{wncd_x_R0-0}{1}: [radius] [21860]: (info): RADIUS:  EAP-Message         [79]     6  ...
{wncd_x_R0-0}{1}: [radius] [21860]: (info): RADIUS:  Message-Authenticator[80]    18  ...
{wncd_x_R0-0}{1}: [radius] [21860]: (info): 01:
{wncd_x_R0-0}{1}: [radius] [21860]: (info): RADIUS:

Tunnel-Private-Group-Id[81]    25  "10_10_30_0-READONLY_VN"

{wncd_x_R0-0}{1}: [radius] [21860]: (info): RADIUS:  EAP-Key-Name        [102]   67  *
{wncd_x_R0-0}{1}: [radius] [21860]: (info): RADIUS:  Vendor, Cisco       [26]    38
{wncd_x_R0-0}{1}: [radius] [21860]: (info): RADIUS:

Cisco AVpair       [1]     32  "cts:security-group-tag=0012-01"

{wncd_x_R0-0}{1}: [radius] [21860]: (info): RADIUS:  Vendor, Cisco       [26]    34
{wncd_x_R0-0}{1}: [radius] [21860]: (info): RADIUS:

Cisco AVpair       [1]     28  "cts:sgt-name=TC2E_Learners"

{wncd_x_R0-0}{1}: [radius] [21860]: (info): RADIUS:  Vendor, Cisco       [26]    26
{wncd_x_R0-0}{1}: [radius] [21860]: (info): RADIUS:   Cisco AVpair       [1]     20  "cts:vn=READONLY_V
{wncd_x_R0-0}{1}: [radius] [21860]: (info): RADIUS:  Vendor, Microsoft   [26]    58
…
{wncd_x_R0-0}{1}: [epm-misc] [21860]: (info): [08be.ac18.c4d9:capwap_9000000a] Username druedahe receiv
{wncd_x_R0-0}{1}: [epm-misc] [21860]: (info): [08be.ac18.c4d9:capwap_9000000a] VN READONLY_VN received
…
{wncd_x_R0-0}{1}: [auth-mgr] [21860]: (info): [08be.ac18.c4d9:capwap_9000000a] User Profile applied suc
```

```
{wncd_x_R0-0}{1}: [client-auth] [21860]: (note): MAC: 08be.ac18.c4d9  ADD MOBILE sent. Client state fla
```

Le WLC envoie ensuite les informations SGT et L2VNID à :

1. Le point d'accès (AP) via CAPWAP (Control and Provisioning of Wireless Access Points).

2. Le protocole Fabric CP via LISP.

Le point d'accès du fabric envoie ensuite la valeur SGT via LISP au fabric EN où le point d'accès est connecté.

Vérification du fabric EN

L'étape suivante consiste à valider si le fabric EN reflète les informations reçues de manière dynamique. La commande show vlan confirme le VLAN associé au L2VNID 8199 :

<#root>

EDGE-01#

show vlan | i 819

1028 Pegasus_APs active Tu0:8196, Gi1/0/4, Gi1/0/5, Gi1/0/6, Gi1/0/10, Gi1/0/18
1030 Pegasus_Read_Only active Tu0:8198, Gi1/0/15

1031 10_10_30_0-READONLY_VN

active

Tu0:8199

, Gi1/0/1, Gi1/0/2, Gi1/0/9

Nous pouvons voir que L2VNID 8199 est mappé au VLAN 1031.

Et la commande show device-tracking database mac <mac address> s'affiche si le client sans fil se trouve sur le VLAN souhaité :

<#root>

EDGE-01#

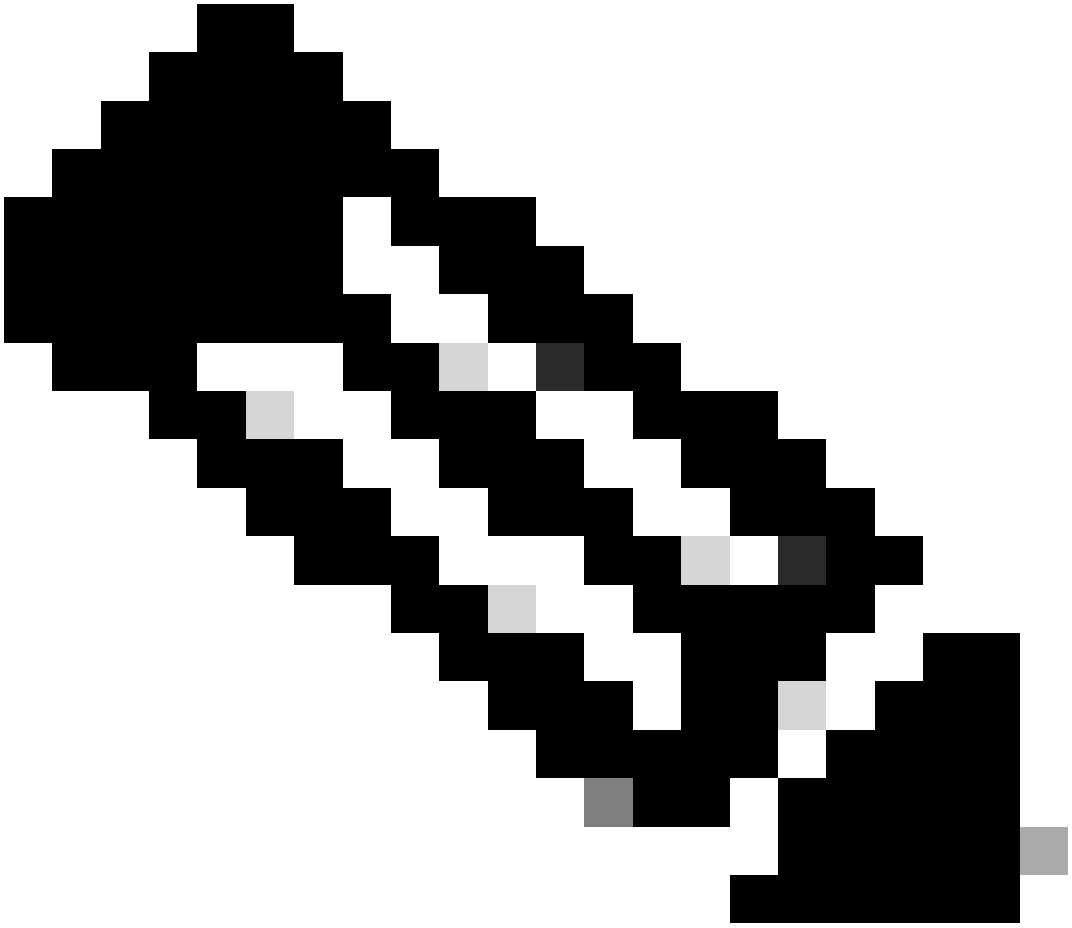
show device-tracking database mac 08be.ac18.c4d9

```
Load for five secs: 1%/0%; one minute: 1%; five minutes: 1%
Time source is NTP, 15:16:09.219 UTC Thu Nov 23 2023
Codes: L - Local, S - Static, ND - Neighbor Discovery, ARP - Address Resolution Protocol, DH4 - IPv4 DH
Preflevel flags (prlvl):
0001:MAC and LLA match     0002:Orig trunk            0004:Orig access
0008:Orig trusted trunk    0010:Orig trusted access   0020:DHCP assigned
0040:Cga authenticated     0080:Cert authenticated    0100:Statically assigned
```

```
    Network Layer Address                   Link Layer Address Interface  vlan  prlvl age    state
macDB has 0 entries for mac 08be.ac18.c4d9,vlan 1028, 0 dynamic
macDB has 2 entries for mac 08be.ac18.c4d9,vlan 1030, 0 dynamic
DH4

10.10.30.12                             08be.ac18.c4d9

     Ac1

1031

  0025  96s    REACHABLE 147 s try 0(691033 s)
```

Enfin, la commande show cts role-based sgt-map vrf <vrf name> all fournit la valeur SGT attribuée au client. Dans cet exemple, le VLAN 1031 fait partie du VRF "READONLY_VN" :

```
<#root>

EDGE-01#

show cts role-based sgt-map vrf READONLY_VN all

Load for five secs: 1%/0%; one minute: 1%; five minutes: 1%
Time source is NTP, 10:54:01.496 UTC Fri Dec 1 2023

Active IPv4-SGT Bindings Information

IP Address              SGT     Source
============================================

10.10.30.12


18

      LOCAL
10.10.30.14             4       LOCAL
```



> Remarque : l'application de la stratégie Cisco TrustSec (CTS) dans un fabric SDA pour clients sans fil (comme pour les clients filaires) est effectuée par les EN, et non par les AP ou le WLC.

L'EN peut ainsi appliquer les politiques configurées pour le SGT spécifié.

Si ces sorties ne sont pas remplies correctement, nous pouvons utiliser la commande debug lisp control-plane all dans l'EN pour vérifier s'il reçoit la notification LISP provenant du WLC :

<#root>

```
378879: Nov 28 18:49:51.376: [MS]  LISP: Session VRF default, Local 172.16.69.68, Peer 172.16.201.4:434
```

wlc mapping-notification

```
 for IID 8199  EID 08be.ac18.c4d9/48  (state: Up, RX 0, TX 0).
378880: Nov 28 18:49:51.376: [XTR] LISP-0 IID 8199 MAC: Map Server 172.16.201.4,
```

WLC Map-Notify for EID 08be.ac18.c4d9

```
 has 0 Host IP records, TTL=1440.
378881: Nov 28 18:49:51.376: [XTR] LISP-0 IID 8199: WLC entry prefix 08be.ac18.c4d9/48 client, Created.
378888: Nov 28 18:49:51.377: [XTR] LISP-0 IID 8199 MAC:
```

SISF event

```
 scheduled Add of client MAC 08be.ac18.c4d9.
378889: Nov 28 18:49:51.377: [XTR] LISP: MAC,
```

SISF L2 table event CREATED for 08be.ac18.c4d9 in Vlan 1031

```
, IfNum 92, old IfNum 0, tunnel ifNum 89.
```

Notez que la notification LISP est d'abord reçue par le PC qui la relaie ensuite à l'EN. L'entrée SISF ou Device-tracking est créée à la réception de cette notification LISP, qui est une partie importante du processus. Vous pouvez également voir cette notification avec :

<#root>

```
EDGE-01#
```

show lisp instance-id 8199 ethernet database wlc clients detail

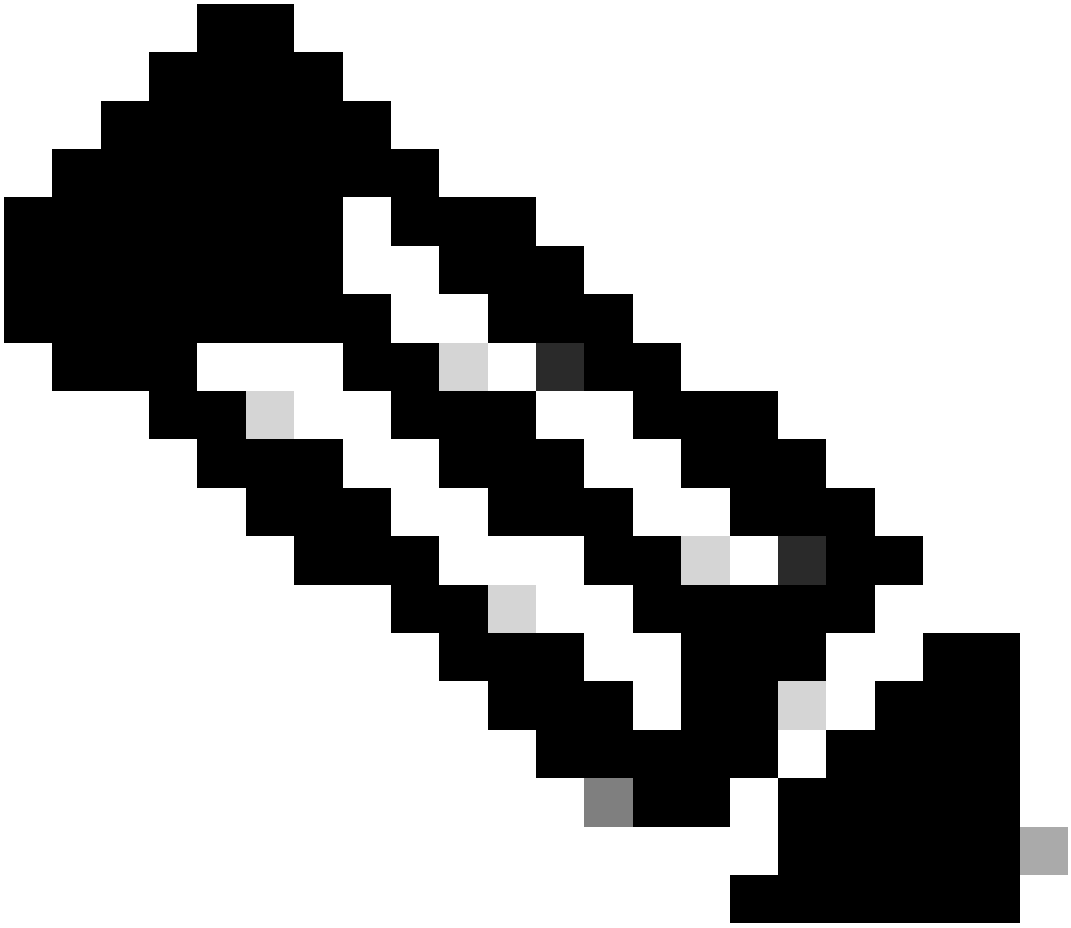
```
Load for five secs: 1%/0%; one minute: 1%; five minutes: 1%
Time source is NTP, 21:23:31.737 UTC Wed Nov 29 2023


WLC clients/access-points information for router lisp 0 IID
```

8199

```
Hardware Address: 08be.ac18.c4d9
Type:             client
Sources:          1
Tunnel Update:    Signalled
Source MS:        172.16.201.4
RLOC:             172.16.69.68
Up time:          00:01:09
Metadata length:  34
Metadata (hex):   00 01 00 22   00 01 00 0C   0A 0A 63 0B   00 00 10 01
                  00 02 00 06   00
```

12

```
 00 03   00 0C 00 00   00 00 65 67
                  AB 7B
```



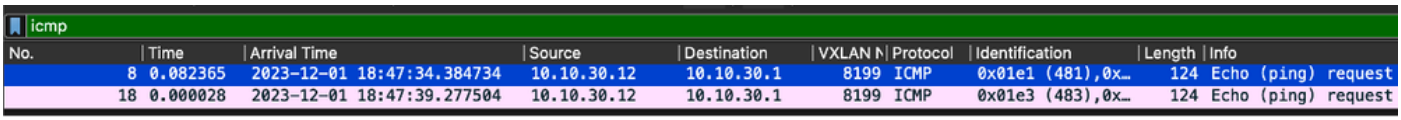
Remarque : la valeur mise en surbrillance 12 dans la section Métadonnées est la version hexadécimale de la SGT 18 que nous avions initialement prévu d'attribuer. Et cela confirme que tout le processus s'est terminé correctement.

Vérification des paquets

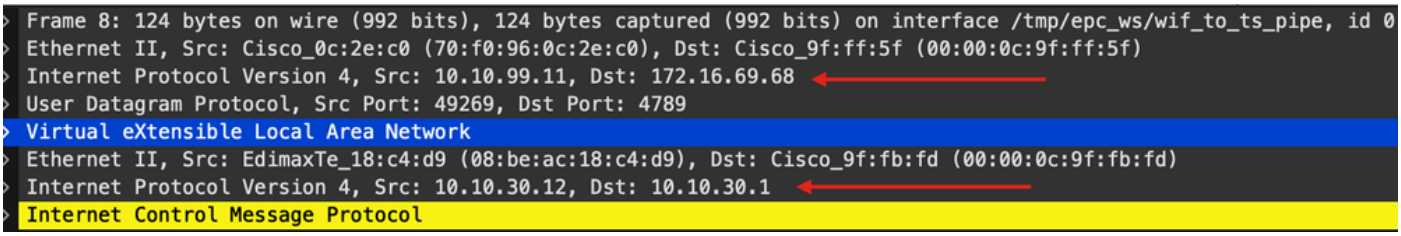
Comme dernière étape de confirmation, nous pouvons également utiliser l'outil Embedded Packet Capture (EPC) dans le commutateur EN et voir comment les paquets de ce client sont transmis par le point d'accès. Pour plus d'informations sur l'obtention d'un fichier de capture avec EPC, reportez-vous à :

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/17-3/configuration_guide/nmgmt/b_173_nmgmt_9300_cg/configuring_packet_capture.html

Pour cet exemple, une requête ping a été lancée sur la passerelle dans le client sans fil lui-même :

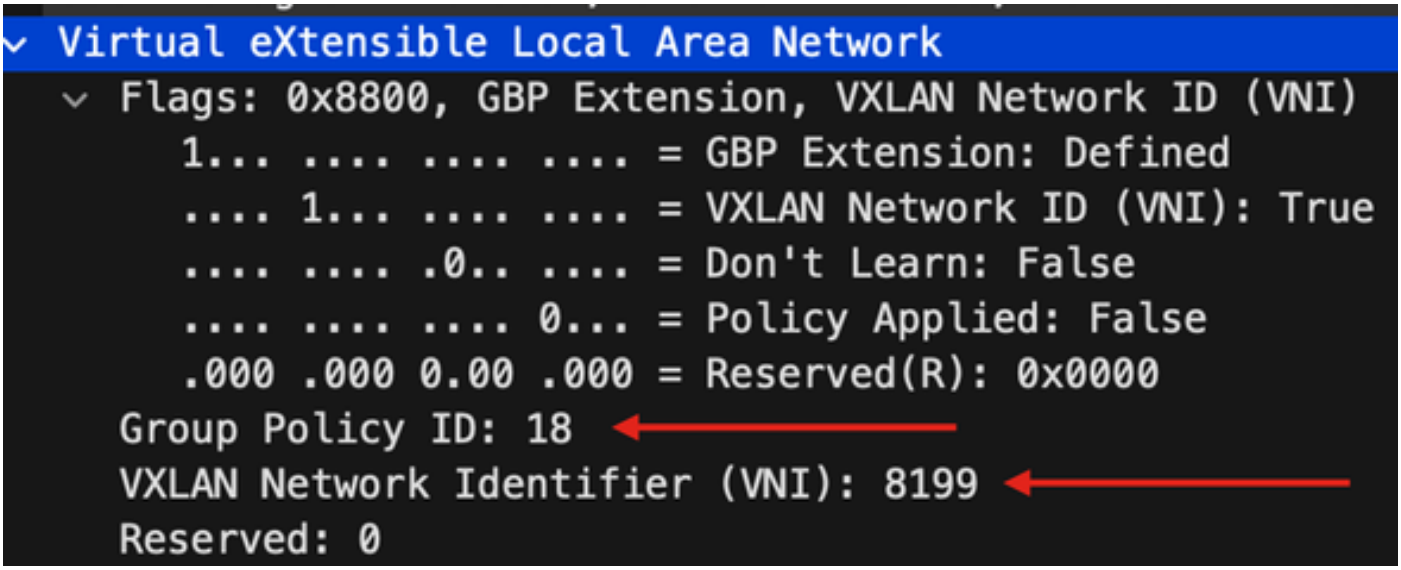


Notez que le paquet doit déjà être fourni avec un en-tête VXLAN du point d'accès, car le point d'accès et l'EN forment un tunnel VXLAN entre eux pour les clients sans fil du fabric :



La source du tunnel est l'adresse IP AP (10.10.99.11) et la destination est l'adresse IP EN Loopback0 (172.16.69.68). À l'intérieur de l'en-tête VXLAN, nous pouvons voir les données réelles du client sans fil, dans ce cas le paquet ICMP.

Enfin, examinez l'en-tête VXLAN :



Notez la valeur SGT en tant qu'ID de stratégie de groupe, dans ce cas, au format ascii et la valeur L2VNID en tant qu'identificateur de réseau VXLAN (VNI).

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.